PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/GB 98/ 02881	24/09/1998	25/09/1997
Applicant		
HALPERN, John, Wolfgang		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 3

   [ ] as suggested by the applicant.

   [X] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

Application No
PCT/GB 98/02881

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAZUE TANAKA ET AL: "KEY DISTRIBUTION SYSTEM FOR MAIL SYSTEMS USING ID-RELATED INFORMATION DIRECTORY" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 10, no. 1, 1 February 1991 (1991-02-01), pages 25-33, XP000209185 ISSN: 0167-4048 page 25, left-hand column, line 1-21 page 26, left-hand column, line 13 - middle column, line 10 page 27, middle column, line 6 - right-hand column, line 17 page 30, middle column, line 7 - page 31, left-hand column, line 8 figure 1 --- -/--	1-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 1999	30/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

1

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 738 058 A (BARKAN MORDHAY) 16 October 1996 (1996-10-16) abstract column 3, line 29 - column 4, line 5 column 7, line 46-57 column 8, line 3-23 column 9, line 10 - column 11, line 21 column 14, line 37-43 column 16, line 17-48	1-15
A	US 5 412 723 A (CANETTI RAN ET AL) 2 May 1995 (1995-05-02) abstract column 1, line 62 - column 2, line 26 claims 4-6	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

Application No
PCT/GB 98/02881

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0738058 A	16-10-1996	US 5864667 A	26-01-1999
US 5412723 A	02-05-1995	EP 0670645 A	06-09-1995
		JP 7250060 A	26-09-1995

QL

3

PATENT COOPERATION TREATY

REC'D 19 JAN 2000

WIPO PCT

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
passtec		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/GB98/02881	24/09/1998	25/09/1997
International Patent Classification (IPC) or national classification and IPC		
H04L29/06		
Applicant		
HALPERN, John, Wolfgang		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 12 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
21/04/1999	14.01.00
Name and mailing address of the international preliminary examining authority:	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Buhleier, R Telephone No. +49 89 2399 8216

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB98/02881

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

3-10	as originally filed	
1,1a,2	with telefax of	20/12/1999

Claims, No.:

14A	filed with the demand	
1-17	with telefax of	20/12/1999

Drawings, sheets:

1/7-7/7	as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

see separate sheet

4. Additional observations, if necessary:

see separate sheet

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

☐ restricted the claims.

☐ paid additional fees.

☐ paid additional fees under protest.

☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

☐ complied with.

☒ not complied with for the following reasons:

see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

☒ all parts.

☐ the parts relating to claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-17
	No: Claims	
Inventive step (IS)	Yes: Claims	1-17
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-17
	No: Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item I

Basis of the report

Item I.3.:

The amendments filed with the International Bureau with the demand under Article 19(1) and with the telefax of 20.12.19999 under Article 34(2) PCT introduce subject-matter which extends beyond the content of the application as filed, contrary to Articles 19(2) PCT and 34(2)(b) PCT. The amendments concerned are the following:

1. The Applicant filed a new dependent Claim labelled No. 14A with the demand. However, the additional features ("parallel outputs of Key registers and Logic Circuit are computer controlled ... preset via a keyboard ... operate in unique synchronism") present in this claim appear to have no basis in the description as originally filed. Hence, no basis for such an extension can be found in the application as filed and thus the claim as filed results in the application being amended in such a way that it contains subject-matter which extends beyond the content of the application as filed, contrary to Article 19(2) PCT.

   Consequently, Claim 14A is not taken into consideration for this International Preliminary Examination Report.

2. Amended Claim 1 specifies that the addresses associated to key numbers are moved at "quasi randomly arranged times for a younger to an older position". However, the originally filed description discloses, that the table with key numbers and associated addresses is update periodically (see page 4, item (6) of key renewal process). Hence, no basis for the amendment is found in the application as filed, contrary to Article 34(2)(b) PCT.

3. Amended Claim 2 defines that the key number replacement routine is implemented prior to the transmission of a new key from the Key Generation Centre and the e-mail stations. However, the originally filed application only discloses that the routine is implemented prior to key transmission from the local server (see page 4, items (6) to (8)). Hence, no basis for the amendment is found in the application as filed, contrary to Article 34(2)(b) PCT.

4. Newly filed Claim 11 introduces the feature of the "real data bits being transmitted at a randomly varying rate, according to the key being used by said e-mail station". No basis for this amendment can be found in the original disclosure where on page 2, §3, it is only specified that the real data is applied with a "delay of one full clock cycle", but no transmission rate is defined (see also description of Fig. 4 on page 5), neither is there a disclosure of the key being involved. Therefore, amended Claim 11 contains subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT.

5. Newly filed Claim 12 introduces the feature of "the automatic server station receives ... the decrypted check number ... calling station". No basis for this amendment can be found in the original disclosure where on page 5, item (10), it is only specified that the random check number is sent to the calling station. Therefore, amended Claim 12 contains subject-matter which extends beyond the content of the application as filed, contrary to Article 34(2)(b) PCT.

6. Amended Claim 12 also defines that the e-mail number is received in encrypted form by the automatic server station. In contrast, the originally filed description discloses that a **dial** number is encrypted and sent to the **distant** server station. Thus, no basis for the newly filed feature can be found in the originally filed application, contrary to Article 34(2)(b) PCT.

7. Amended Claim 13 states that the pattern diffusion is applied according to the new encryption key. However, no basis for this feature can be found in the originally filed application (see originally filed Claim 11), contrary to Article 34(2)(b) PCT.

Item I.4.:

Concerning the Applicant's request for sending supplementary drawings filed with letter of 15 May 1999, it is noted that no supplementary drawings were filed during the international preliminary examination procedure.

Re Item IV

Lack of unity of invention

1. The International Preliminary Examining Authority is of the opinion that two groups of potential inventions are claimed in the present application. This opinion is based on the following reasons:

The lack of unity becomes apparent a priori, i.e. before taking the prior art cited in the International Search Report into consideration (see PCT Guidelines III-7.5).

The separate groups of potential inventions are:

Group 1: Claims 1 - 11 and 13 - 17
Encryption and automatic key renewal systems for associating address codes to keys, associating key age, issuing new keys prior to e-mail stations and maintaining a look-up table of valid key numbers by date and address code.

Group 2: Claim 12
Encryption and automatic key renewal system incorporating a key replacement routine whereby keys are encrypted with themselves and random check numbers are added in encrypted form for authentification of a user whishing to establish a secure communication.

The common feature "encryption and automatic key renewal system" of the two groups of potential inventions is widely known in the art.

The potential remaining special technical features of these different sets of potential inventions are not the same. They are not corresponding either, since they are based on different concepts.

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The following documents are referred to:

   D1: EP-A-0 738 058 (BARKAN MORDHAY) 16 October 1996
   D2: US-A-5 412 723 (CANETTI RAN ET AL) 2 May 1995
   D3: KAZUE TANAKA ET AL: 'KEY DISTRIBUTION SYSTEM FOR MAIL SYSTEMS USING ID-RELATED INFORMATION DIRECTORY' COM- PUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 10, no. 1, 1 February 1991 (1991-02-01), pages 25-33, ISSN: 0167-4048

2. Present Claim 1 is in accordance with the requirements of Article 33(3) PCT because its subject-matter is novel and inventive.

   The claim relates to an encryption and automatic key renewal system for confidential e-mail communication. Similar systems are known from document D1 which discloses a key generation centre for the generation of random keys for the use of the e-mail stations; means for renewal of the keys; scrambling means for encrypting transmission of data; and local server stations which store and update the random keys generated in the key generation centre, whereby the keys have associated access codes and time flags indicating the issue age of each key.

   The main problem to be solved is regarded as to provide enhanced security for data transmission between user-controlled e-mail stations.

   This is solved in that prior to each confidential communication to be set up between two e-mails stations, a new encryption key to be used is sent from the local server to the sending e-mail station. Furthermore, the look-up table which stores the keys at the local server is updated automatically from the key generation centre, whereby the oldest keys are replaced by new keys.

   The solution is not suggested by the teaching of D1 because in the system

according to D1 a private/public key encryption technique is used, whereby a permanent private key is kept at the e-mail stations and a public key is used at the local server for further encrypting encrypted data sent from the e-mail stations. There is no possibility disclosed in D1 to automatically renew the encryption key used at the e-mail station prior to each communication. Furthermore, the public keys at the local servers in the system of D1 are updated only on user request and not automatically from a key generation centre as in the system according o Claim 1. Additionally, D1 does not specify details of list-keeping and updating the list of keys.

Hence, the teaching of D1 is several non-obvious steps away from the inventive solution.

Document D2 does not disclose or suggest the inventive solution because in the system of D2 new keys are calculated directly at the e-mail stations and not served from the servers as specified in Claim 1. Furthermore, at the servers keys are calculated in a distributed manner and not received from a key generation centre. Hence, the teaching of D2 is far away from the subject-matter of Claim 1.

Document D3 also does neither disclose nor suggest the inventive solution, because in the system of D3, new keys are generated at the e-mail stations based on a user secret which is generated at a trusted centre. No information is found in D3 about updating the user secret. Hence, the teaching of D2 is also far away from the subject-matter of Claim 1.

3. Claim 13 is also in accordance with Article 33(1) PCT because its subject-matter relates to an automatic key renewal system wherein, as in accordance with the inventive feature of Claim 1, the e-mail stations are automatically provided with new encryption keys prior to each confidential communication. Furthermore Claim 13 specifies the random key generators of which the functional features are neither disclosed nor suggested by document D1.

4. The dependent Claims 1-11 and 14-17 relate to optional features of inventive Claims 1 and 13. Hence their subject-matter is also novel and inventive.

5. Independent Claim 12, in so far as it can be understood and fulfills Article 34(2)(b) PCT, appears to fulfill the requirements of Article 33(1) PCT, because the claim relates to an encryption and automatic key renewal system wherein a single key is encrypted with itself and a random check number is added in encrypted form for authentification of an e-mail station whishing to establish a secure communication via a server to another e-mail station.

These features are neither disclosed nor suggested by document D1, because in the authentification routine of D1 two private/public key pairs but no check numbers are used. Hence, the teaching of D1 is far away from the inventive features of Claim 12.

Documents D2 and D3 do not address authentification procedures in detail.

Re Item VII

Certain defects in the international application

1. The preamble of independent Claim 1 does not contain the following feature, which is also known from document D1 (Rule 6.3(b) PCT):

   "said local server stations store said keys in a look-up table (column 3, lines 29-33), each key being associated with an address code (column 3, lines 49-56; and column 22, lines 8-9) and each address code having an associated data indicative of the age of said key at any time and to classify the age relative to the age of other keys in use at any given time (see "issue date", column 23, lines 15-18 and lines 32-36).

2. The features of Claims 1, 12 and 13 are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT). This applies both to the preamble and characterising part of the claims.

3. Contrary to the requirements of Rule 5.1(a)(iii) PCT, the description is not adapted to the wording of the independent Claim 12.

4. According to the requirements of Rule 11.13(l) reference signs not appearing in the description shall not appear in the drawings, and vice versa. This requirement is not met in particular in view of many of the reference signs in Figs. 5-10.

Re Item VIII

Certain observations on the international application

1. Claim 1 specifies an address code and access addresses. It is unclear whether these terms represent the same addresses, or whether the address code is an e-mail address.

2. Entity Claim 1 also defines method steps ("wherein ... addresses can be moved ... and oldest numbers being relegated"). It is unclear which functional features of the system are adapted to perform these operations. Hence, the category of the claim is unclear.

3. System Claim 5 contains a method step ("the server station acts as a switch-board"). Hence, the category of the claim is unclear.

4. System Claim 7 defines the algorithm used for the encryption process. Thus, the category of the claim is unclear.

5. Also the category of system Claim 8 is unclear. By referring to time schedules, the claim specifies method steps: a "precise point in time for switching...". It is unclear which means functionally define the point in time.

6. Claim 9 should not contain technical features in brackets (see Guidelines PCT/GL/3 III, 4.11).

7. Claim 12 lacks clarity because with the wording: "In an encryption ... system ... a key replacement routine", it can be queried whether the claim is directed either to a system, or to a process. Thus, the subject-matter and the category of the claim is unclear.

8. System Claims 14 and 15 define encryption operations and processes which are continually influenced and modified. Hence, the category of these claims is unclear.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

To:
Halpern, John Wolfgang
15 Jordan Court
Imgram Cresent W
Hove BN3 5NUEast Sussex
UNITED KINGDOM

Applicant's or agent's file reference	Date of mailing *(day/month/year)* 30/08/1999
	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/GB 98/ 02881	International filing date *(day/month/year)* 24/09/1998
Applicant HALPERN, John, Wolfgang	

1. [X] The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Fascimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

[ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

[ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Theresia Van Deursen

EL721435571US

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international pbulication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PAT T COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

HUGHES, ANDREA
Frank B. Dehn & Co.
179 Victoria Street
London EC4V 4EL
ROYAUME-UNI

Date of mailing (day/month/year)
18 February 2000 (18.02.00)

Applicant's or agent's file reference

IMPORTANT NOTIFICATION

International application No.
PCT/GB98/02881

International filing date (day/month/year)
24 September 1998 (24.09.98)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address

State of Nationality | State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [X] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
HUGHES, ANDREA
Frank B. Dehn & Co.
179 Victoria Street
London EC4V 4EL
United Kingdom

State of Nationality | State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:
The above-mentioned agent has taken over representation.

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
G. Bähr

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 31 May 1999 (31.05.99)	
International application No. PCT/GB98/02881	**Applicant's or agent's file reference**
International filing date (day/month/year) 24 September 1998 (24.09.98)	**Priority date** (day/month/year) 25 September 1997 (25.09.97)
Applicant HALPERN, John, Wolfgang	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

21 April 1999 (21.04.99)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

N. Lindner

Telephone No.: (41-22) 338.83.38

A Data Encryption System for Internet Communication

There is a general concensus that serious use of the internet potential for the needs of Commerce and Industry requires a 100% long-term effective system for protecting privacy of the interchanges.

Several aspects apart from privacy would be important in making a choice of the technique. It would have to be suitable for all digital transmissions, irrespective of the coding employed. The same encryption system should be workkable for lettered, audible or visual messages. Also, the time of processing the data should preferably not add more than 80% to the time for transmitting the same data in the clear form. Furthermore, no time should be spent on looking up directories for keys or other procedure rules.

The objectives of this patent application follow from what has just been said:

- to create for owners of PC's certain supplementary components easily added with the result of replacing registered and high-priority mail transmissions by a less expensive and faster track protected against breach of confidentiality.
- to reduce the need for personal trustworthiness and to replace it by trustworthiness of the provisions of the system.
- While the idea of "trusted third parties" is appropriate where Government interests are directly involved, the many contingencies that arise when applied to all communications would strain an already overburdened legal system. In contradistinction, the here proposed method would save trustworthy server stations from slipping into arbitrariness, favoritism and self-serving bureaucracy. At the same time it would open a clear route for observers at Govenment level to use their authority of sampling messages in the interest of crime prevention and to do so even for longer periods if and when properly authorized and reasoned for in exposés open for public inspection within six years.

This paper will outline the t e c h n i c a l p l a t f o r m for accomplishing the above sketched objectives, with the further provision that its service be available to everyone at a relatively low extra cost over and above the cost of using internet communication.

The said 'technical platform' constitutes a system resting on two main pillars, namely

(a) an algorithm which generates variable wordlength data scrambling

(b) a hierarchic system of key distribution (e.g. a regulated method for ageing and then eliminating keys)

In place of a lengthy explanation, we begin by referring to Figure 4 which illustrates the idea of variable word length text transformation. It will be clear that computerised scanning of the encrypted text will in this case have no prospect of providing any clue.

Figure 5 shows a functional block diagram of the encryption/decryption hardware. In early implementations, a 16 bit shift register was used (block SR) with simple output to input connection. The encrypted output resulting from such an arrangement showed a certain periodicity if the clear text consisted of the binary representation of a single letter, for example the letter 'a' in unchanging repetition. This revealed the potential for a certain weakness of the method unless steps are taken to overcome this possible point of attack for a hacker. In present designs we use a 31 bit shift register as the basis for a pseudo random data generator wherein the periodicity is vastly (pattern recurrance only once every 2,14 billion different combinations) reduced. In addition, further measures are taken to begin each message with an undefined length of meaningless text. That text is not delivered in clear by the algorithm. For the user it constitutes simply a few seconds waiting time added to the setting up time. One method of achieving this will be explained in conjunction with Figures 3,4 and 8.

Returning to the description of Fig. 5, paralell outputs from the shift register are connected to various logic elements under the heading LOGIC CONTROL. This comprises for example, a programmable counter, several flip flops and bistables and various gates. Some of the logic control elements are also exposed to inputs of the logic levels of the real data, both outgoing or incoming. These data are applied with a delay of one full clock pulse duration. This is done in the squares named 'bit delay'. The encrypted text on line 1_2 is derived from an OR gate into which alternately pass bit elements from the real data and from the Random data generator RDG, respectively a, by real data modified,output from said generator. Encrypted data received are descrambled by action of the Logic Control group, in a single AND gate.

Figures 6 and 7 explain how it is possible to have 8 - 10 simultaneously valid keys and how they are weighted in a number ageing process. Figure 8 shows a functional block diagram of an LSI chip such as would be capable of carrying out data encryption at a high clock rate suitable for any communication network and would provide added security over and above the basic scheme of Figure 5.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :		(11) International Publication Number:
H04K	**A2**	**WO 99/16199**
		(43) International Publication Date: 1 April 1999 (01.04.99)

(21) International Application Number: PCT/GB98/02881

(22) International Filing Date: 24 September 1998 (24.09.98)

(30) Priority Data:

9720478.8	25 September 1997 (25.09.97)	GB
9820824.2	24 September 1998 (24.09.98)	GB

(71)(72) Applicant and Inventor: HALPERN, John, Wolfgang [GB/GB]; 15 Jordan Court, Imgram Crescent W., Hove, East Sussex BN3 5NU (GB).

(81) Designated States: PL, PT, RU, SE, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: A DATA ENCRYPTION SYSTEM FOR INTERNET COMMUNICATION

(57) Abstract

Two versions of a variable word length encryption method are discussed adapted for providing the means for long–term confidential transmission of printed characters, pictures, and voice dialogues over the telephone lines or the internet.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A Data Encryption System for Internet Communication

There is a general concensus that serious use of the internet potential for the needs of Commerce and Industry requires a 100% long-term effective system for protecting privacy of the interchanges.
Several aspects apart from privacy would be important in making a choice of the technique. It would have to be suitable for all digital transmissions, irrespective of the coding employed. The same encryption system should be workkable for lettered, audible or visual messages. Also, the time of processing the data should preferably not add more than 80% to the time for transmitting the same data in the clear form. Furthermore, no time should be spent on looking up directories for keys or other procedure rules.
The objectives of this patent application follow from what has just been said:

- to create for owners of PC's certain supplementary components easily added with the result of replacing registered and high-priority mail transmissions by a less expensive and faster track protected against breach of confidentiality.
- to reduce the need for personal trustworthiness and to replace it by trustworthiness of the provisions of the system.
- While the idea of "trusted third parties" is appropriate where Government interests are directly involved, the many contingencies that arise when applied to all communications would strain an already overburdened legal system. In contradistinction, the here proposed method would save trustworthy server stations from slipping into arbitrariness, favoritism and self-serving bureaucracy. At the same time it would open a clear route for observers at Govenment level to use their authority of sampling messages in the interest of crime prevention and to do so even for longer periods if and when properly authorized and reasoned for in exposés open for public inspection within six years.

This paper will outline the t e c h n i c a l p l a t f o r m for accomplishing the above sketched objectives, with the further provision that its service be available to everyone at a relatively low extra cost over and above the cost of using internet communication.

The said 'technical platform' constitutes a system resting on two main pillars, namely

(a) an algorithm which generates variable wordlength data scrambling

(b) a hierarchic system of key distribution (e.g. a regulated method for ageing and then eliminating keys)

In place of a lengthy explanation, we begin by referring to Figure 4 which illustrates the idea of variable word length text transformation. It will be clear that computerised scanning of the encrypted text will in this case have no prospect of providing any clue.

Figure 5 shows a functional block diagram of the encryption/decryption hardware. In early implementations, a 16 bit shift register was used (block SR) with simple output to input connection. The encrypted output resulting from such an arrangement showed a certain periodicity if the clear text consisted of the binary representation of a single letter, for example the letter 'a' in unchanging repetition. This revealed the potential for a certain weakness of the method unless steps are taken to overcome this possible point of attack for a hacker. In present designs we use a 31 bit shift register as the basis for a pseudo random data generator wherein the periodicity is vastly (pattern recurrance only once every 2,14 billion different combinations) reduced. In addition, further measures are taken to begin each message with an undefined length of meaningless text. That text is not delivered in clear by the algorithm. For the user it constitutes simply a few seconds waiting time added to the setting up time. One method of achieving this will be explained in conjunction with Figures 3,4 and 8.

Returning to the description of Fig. 5, paralell outputs from the shift register are connected to various logic elements under the heading LOGIC CONTROL. This comprises for example, a programmable counter, several flip flops and bistables and various gates. Some of the logic control elements are also exposed to inputs of the logic levels of the real data, both outgoing or incoming. These data are applied with a delay of one full clock pulse duration. This is done in the squares named 'bit delay'. The encrypted text on line l_2 is derived from an OR gate into which alternately pass bit elements from the real data and from the Random data generator RDG, respectively a, by real data modified,output from said generator. Encrypted data received are descrambled by action of the Logic Control group, in a single AND gate.

Figures 6 and 7 explain how it is possible to have 8 - 10 simultaneously valid keys and how they are weighted in a number ageing process. Figure 8 shows a functional block diagram of an LSI chip such as would be capable of carrying out data encryption at a high clock rate suitable for any communication network and would provide added security over and above the basic scheme of Figure 5.

Detailed Discussion of the Drawings

FIG. 1 shows two personal computers or communication work stations using a fixed secret key, or using a program permitting one of the stations to utilize the encryption key of the other.

FIG. 2 illustrates a situation where the official key employed within an organisation is not normally used for the actual encryption/decryption of data. If for example station A represents the word processor in a secretarial pool of one company, and station B the processor office in another company, And the message sender has a small computer in his office A_p wishing to send a confidential message to a particular person having a computer B_p , then the procedure would be as follows:

(a) The secretary at A will type into the word processor A a statement from Mr. A_p in clear language and put it on disk.

(b) Next, the secretary agrees with A_p to display on the window of A_p the text as written for approval or amendments.

(c) When approved, A_p will contact the secretary at A over the phone to prepare internet connection with the communication of office at B.

(d) When communication is established, the secretary rings A_p to report 'ready'.

(e) The executive at A_p now types his private password ppw into his keyboard thereby transmitting it to work station A where the instruction code tells the computer to deduct (or add) the password number, or a multiple thereof, from the encryption key of the organisation.

(f) Once this is done a green light informs the secretary that the clear text derived from the disk is to be moved through the encryption algorithm and out into the internet.

(g) The encrypted message is taken on disk at computer unit B. It cannot be read by staff.

(h) When executive B_p returns to his office, he will find a light signal indicating that he has a personal message. Accordingly, he will enter the agreed pass word ppw on his computer keyboard together with the instruction of deducting it from the common general key. After that, the decrypted message will appear on the screen B_p.

It would be technically possible to provide the Managing Chief in each company with an automatic printout of all personal messages, to enforce the sharing of confidential information.

Since the encryption system here expounded is not primarily determined by mathematical conversions, and therefore all numbers are equally suitable, it would suffice if the executives concerned are told that they must have a six-digit ppw. Knoledge of agreed passwords may therefore be limited to the parties themselves.

FIG. 3 shows the structure of a Service Center SC for almost fully automatic connection service to clients wishing to send messages required to remain confidential. Fig.3 shows again a workstation A in one locality and another workstation in a remote locality but using the same equipment. The central server station consists of two sections (A & B). These sections comprise channel switching section sw, switch control sections LS_A or LS_B; Two algorithmic sections virtually identically with those shown for example in Fig. 8; In each section is also a key register for storing a key K_n and a random text data holding register D_r. Below is a computing section COMP, and below that a memory of past transactions, M. The computer unit COMP has a preferably direct link with a National Key Generator Center NKGC. Where a direct link is not available, a switched connection with NKGC will do because no clear data are passed through this link. (see also Fig. 6) The process prior to A sending a confidential message to B, can be reported in ten steps.

(1) station A dials the local Service Center (SC) and immediately thereafter dials also the number of the desired receipient B.

(2) Station A gets indication that connection is made

(3) prompted by (2), section A receives from station A the address code for identifying the key held at present by station A. (see address reg., fig.7).

(4) section B of SC calls station B.

(5) Station B responds by sending its address in clear

(6) using the two address numbers from A and B, the SC looks up from a memory table similar to that of Fig. 7 the at the time valid secret key numbers. Section A of SC extracts the key nr. for station A, inserts it into the algorithm (algo) thereby encrypting K_A by K_A and sends it to station A for verification. - Section B of SC proceeds likewise with station B. (the table is stored in section COMP, and is periodically updated from the national key generator centre, see Fig. 6).

(7) A and B receive the encrypted keys K_A' and K_B' respectively, decrypt them with their respective K_A and K_B keys, and if any station cannot verify it sends to the respective section of SC a repeat request. If this also fails ... a 'failed' signal in clear goes to both stations.

(8) With both comparisons correct, the SC proceeds to obtain from its COMP section an alternative key number K_C which section A encrypts with K_A, and section B encrypts with K_B, and sends these numbers to stations A and B respectively where they are decrypted and entered into their key registers, substituting their earlier keys.

(9) Stations A and B send out K_c' to the respective sections of SC where they are compared to test equality.

at this point both stations would be ready to communicate. The time lapse so far (after the initial dialling by station A) would be less than 4 seconds. To improve security further a further step is adding a few seconds to the setting up procedure:

(10) The Computer Resource Unit COMP supplies to the operative sections a random number called D_r where it is entered into a register connected for generating through re-circulation a fairly large pseudo random number. This number is continually passed through tha algo sections of SC, and the output is sent to stations A and B where they are decrypted and continually passed through a comparator register being only a few bits (5 - 12) long. Paralell outputs from this register are continually compared with a similar number of selected paralell bit outputs from the larger, in the opposite sense rotating, key register. Whenever all the bit positions of the static bit comparator are at the strobing moment equal, a pulse is released both in the stations A and B and in the Server Center SC internally which stops the D_r bit generator and establishes in the switching sections sw a direct connection between A and B.

It should be noted that the true time distance in terms of real data clock pulses could not be determined by a hacker and therefore no conclusion be drawn as to the number structure of the initial key in the key register of the algorithm. This is because the variable word length encryption applies also to the D_r data stream transmission.

Figure 4 illustrates the nature of an encrypted message consisting as it does of an initial phase of random data the length of which cannot be externally detected, and a transmission phase consisting of a quasi-random mixture of real data bits and random bits - all in a single undivided string of bits giving no clue where one word begins or ends. There is thus no reference points against which an analyst might be able to study the bit sequences.

Figure 5 has already been adequately dealt with on page 2

FIGURE 6 explains the role of the N K G C (national key generator center). In that Center the K_n numbers with their address allocations, and also the D_r numbers are generated and the protocol for the transfer of these numbers to head offices of various kind is observed. The management of the Center would be limited to determining the optimum rate at which updates for new numbers should be made. This would be set responsive to the performance of the system as a whole as reported by supervisors. Performance reports from head offices such as Bk (banks) or TR (transport organisations) or SC's (service centers for confidential communications) would be studied by supervisors and appropriate responses formulated. Management would have no access to actual key numbers. When a station mal-performs, its encryption module is detached and sent to the factory,and replaced by a factory-new one.

It is here suggested that both systemwise and with respect to the encryption module IC, the here explained confidential message system may be used also in bank transaction as also in remotely issued travel passes and routing instructions.

FIGURE 7. This table surveys the position changes of a number which ranges from a nascent phase to an active, semi-active, and finally abandoned phase. The numbers are classified in terms of age. The active number range comprises in this example five ageing positions, and so does the semi-active range of numbers. If each column segment represents the time span of, say, one week, it would take ten weeks for a number to travel from the nascent region through the active and semi-active region, in order to exit into the for normal use inaccessable abandoned region.
Once an address is allocated to a number, the two numbers remain associated during their migration through said regions.
Both active and semi-active numbers are valid numbers, and are therefore accepted by terminals and server stations for commencing a communication. However, either right at the beginning or after completion of the communication event, an older active number is substituted by a younger one, or any semi-active number is substituted by any number from the active region. If an internet station, or an IC card - through non-useage over a longer period of time - has in its encryption algorithm a number which at the time of re-use belongs to an abandoned number, it would be necessary to make contact with certain supervisory organs which have at their disposal access to a central register which keeps a record of numbers abandoned in the past. Such organs would be allowed to make also additional checks before they override the absence of a valid key number and bring the station or card up to date again.

FIGURE 8 This shows an example for the LSI chip circuit block diagram. A chip of this type would be needed in an extension card for insertion in one of the the slots for extension functions, such as are common in personal computers. The following are the main features of the Chip:

The four clock phases needed to operate the circuit may be either on chip generated or supplied by the Computer (as fig. 8 indicates). The chip would also be used in the Service Center SC. There is a STORED KEY VERIFICATION AND KEY EXCHANGE MODULE (1). This group has four input lines (ROP, CK2, $\overline{En}$ and password ..) and two output lines En & K. In connection with internet operation there may be at least one more input from outside the chip, when namely the output EN has to be delayed because of delays, in getting a connection completed or for whatever other reason. When the electric level at EN changes this indicates that verification and key exchange are satisfactorily completed, and, with everything else being ready the next phase can begin. - The ROP input to module 1 resets all internal bistables and occurs when power is switched on or shortly afterwards. The d-input is connected to the incoming signal line to enable the address reference for the encryption key held, to be read out . This last mentioned detail is not shown worked out in figure 8.

In practice, the circuit must satisfy the condition that external communication of keys must take place only in the encrypted form. The input CK2 provides the proper clock phase for the key exchange functions. The output K transfers to block 2 the new key before commencing the encryption and decryption functions. All encrypted incoming line signals are decrypted by gate 16.

The pseudo random key generator rotates the shift register 2 with every CK3 clock pulse. The programmable counter 4 is advanced with every $\overline{CK3}$ clock pulse. The bistable 23 is reset with every CK2 clock pulse. The programmable counter , after producing a carry output is loaded with the paralell output from the key generator at the time, that is between CK3 and the following CK2. The incoming or outgoing real data bits also have an effect on the constellation of the logic interconnections, block 3 in that the consecutive data bits are fed with the delay of one complete clock cycle to block 3. From this arrangement it follows that discovery of the clear text is not possible without the prior knowledge of the clear text, making discovery superfluous. Text generated in the P C is connected to a buffer register (17), or perhaps two such registers, via the terminal d_o The buffer fills until a signal F (full) is fed back to the computer. As the buffer clears due to passing on data to gate 14, the buffer register is filled up again from an overflow register in the computer itself.

The job of the pseudo random data generator, block 11, is to provide meaningless data bits to be fed to outlet 'd' via the gates 12 and 13 when $\overline{c}$ is high. The gate 14 admits data from the buffer 17 only when c is high. As the bistable outputs c and $\overline{c}$ are dependent on the rest of the algorithm, a quasi random mixture of real and fake data is produced at the d output when in the sending phase. When in the receiving phase, the scrambled mixture of real and random data bits is descrambled by gate 16. The remaining real data in the gate 16 output are channeled in the very beginning before the actual message transmission to gate 21 and to the d input to block 1 during the initial key checking and exchanging phase. The output from 21 feeds into a short shift register 7 which has paralell outputs for each of the bits it holds. These are applied to a static comparator 8 and compared bit by bit with an equal number of outputs from the register of block 2. As both the registers are shifted on the rising edge of CK3 but in opposite directions this has the effect of scanning and testing the registers as to the chance of hitting a seven bit (or 5-bit, etc.) combination where all the input bit comparisons are successful causing an output pulse by the strobing clock CK4 on AND gate 9 to trigger bistable 10. As the gate of 16b is enabled by $\overline{Q}$, with the disappearance of this high level the flow of encrypted nonsense data stops. A very similar arrangement in the Service Center SC also causes the flow of these data to stop and to connect the station A (Fig. 3)with station B directly via switch elements sw. From now on, encrypted data are meaningful text from A to B. Station B will from that moment on channel data received at d (Fig. 8) through gates 16 and 16a to the output interface d_i on the PCB whose adge contactors are plugged into the appropriate sockets inside the P C. When the workstation PC sends, an output SE is generated which disables the gate 16a. The computer can also generate a signal along chip input pwl (password line) to modify the encryption key as explained in connection with the comment on Figure 2.

Finally, the question should be addressed whether the present encryption system permits the communicating parties to engage in a dialogue. The answer is yes, messages may be sent in both directions with or without pause and there is no limit to the length of the message or of the dialogue.

Because of the nature of the encryptotion method which defies any form of systematic factoring of the encrypted text, it is unlikely that a free-lance hacker can be a threat to the described system in spite of the fact that the interchnages between the Client Computer (CC) and the Server Station (SSt) contain one element, the address information, in the clear. In a slightly better position are the expert engineers of the server stations which may have an insight into the precise moment when within the encrypted data flow various addresses are offered. In a very general way one may admit the possibility of a problem that may then arise.An alternative scheme would permit also the address code to be sent only in the encrypted form. According to our proposal, the Client Computers of a local region would have a special relationship with the Internet Secure Server station of that same region (SSt). The Client Computer (CC, Fig. 9) would when contacting the Server send to it its ID number.This number serves as an address in the Server station's memory bank which would contain the very same data as the Client station, namely

a chip serial nr. and / or the date of inauguration of the client chip (from an unalterable ROM).
the last entered encryption Key nr.
The last entered Preamble Delay nr. D_r
and in place of a revolving address code, an annual sequential entry serial nr.

Based on this information, the calling station may immediately begin with sending its own data in encrypted form which the receiving Server station would place into a comparator register, and if all these data are correct will automatically issue a new key number and preamble random delay number and the next sequential nr., in encrypted form using the old key, and the corresponding decrypted clear data are then placed into the memory of the Client Computer station. Its operator is requested to dial the distant station to which message material is to be sent. The dial number would pass through the encryption algorithm and therefor does not allow a third party to know which company or person will be connected. The first part of the dial code will call up the distant Server station (for example BBZ) and the number part will call up the particula CC, say 1500. When the latter responds, it sends its own ID number to the distant local Server station, and a similar comparison process as described above, is initiated. If this verifies that the correct CC station has been contacted, the new key (K_{n2}) given to the calling station is now also given to the called station. After this is verified, this is made known to the calling station, and a display invites its operator to proceed sending the intended material (text, drawings, voiced comment, etc).

The just described alternative logistics for a variable word length data transmission system, would blend well into telephone and internet based communication infra structures.

It is feasible that just one further step in this direction could be made by integrating the envisaged function of secure Server Stations with the location of telephone branch Exchanges (as indicated in Figure 10), This would be economical in installation costs,and could work fully automatically in the environment of an automatic switching system. This does not exclude the computerized electronic equipment being housed in a separate reinforced building. It would suffice to have that building in close vicinity to the said telephone Exchange station.

C L A I M S

1. An encryption and automatic key renewal system for confidential E-Mail comprising at least one E-mail station or internet computer linked to a communication system
a national center for the generation of random keys for the use of said stations,
means for the scrambling or encrypting of data in said stations,
means for the periodic renewal of keys controling said scrambling means and local server centers which store and update the said random keys generated in said national center,
WHEREIN said keys shortly before they are delivered from the said Center become associated with one of a limited number of address codes, and
WHEREIN the number of the week within a year or some other flag data are attached to said address code that will readily permit the evaluation of the age of said key at any time and to classify its age relative to the age of other keys in use at a given time, and
WHEREIN FURTHER a server station when issuing the youngest number to an internet station will delete the oldest number from its current list of valid key numbers and utilise the former address code of that abandoned key for associating it with the youngest key (Fig. 7).

2. An encryption and automatic key renewal system for confidential E-mail as in CLAIM 1
WHEREIN the procedure for recognising the legitimacy of a Server Station by a calling E-mail station is as follows:
(a) sending to the server station the address code attached to its own encryption key
(b) the address must assist the server station in obtaining the calling station's encryption key
(c) The Server station equipment encrypts that key number by itself
(d) the Server station sends th encrypted key to the E-mail station
(e) the E-mail station decrypts using its own key and places the result into a comparator register
(f) If the compared numbers are equal, the E-mail equipment informs the Server sttaion accordingly (FIG. 7).

3. An encryption and automatic key renewal system for confidential E-mail as in Claim 2, WHEREIN in the case of receiving the OK signal the Server station is programmed to obtain from its computer section (COMP) an alternative key number (K_C) from the current valid list of key numbers, and to encrypt that new number with the key of the calling station, and wherein the latter is programmed upon receipt of the encrypted new key to decrypt said number and to place it into its key register in substitution of the number it had before.

4. An encryption and automatic key renewal system for confidential E-mail as in Claim 3, WHEREIN the Server station ($SC_{(A)}$), Fig. 3, also acts as an Switchboard for connecting a calling station to a requested receiving station (B), and WHEREIN the Server station consists of a twin structure which is equipped with two sets of encryption algorithm (algo), two sets of switching controls, (LSA and LSB), and two sets of buffer memories (K_n) for holding key number, address codes and other relevant flags as supplied by the computer section COMP.

5. An encryption and automatic key renewal system for confidential E-mail as in any preceding Claim
WHEREIN the said twin sections of the said Server Center equipment (SC) also contains a pseudo-random generator register (D_r) in order to generate quasi-data inputs of equal length simultaneously transmitted and encrypted by the said K_C number to the communicating stations (A,B) in order thereby to shift the starting conditions in the algorithms of the E-mail units for the real text (see Fig. 4) to an undetectable point.

6. An encryption and automatic key renewal system for confidential E-mail as in claims 1 - 5 wherein the algorithms used for the encrypting process produce word-bit configurations consisting of more than 8 bits and less than 16 bits per word transmitted , and the bit number per word is continually changing.

7. An encryption and automatic key renewal system for confidential E-Mail as in CLAIM 5, WHEREIN the precise point in time for switching the communicating stations from the said initial meaningless random information (being received but not in its decrypted form outputted) is functionally defined by comparing the data flow in two registers, namely register 2 with that of register 7 whereby the data shift is prompted by the same clock phase (CK3) but occurs in opposite directions.

8. An encryption and automatic key renewal system for confidential E-Mail as in any of the preceding claims,
WHEREIN the main circuit groups of the integrated algorithm circuit (FIG. 8) comprises

(a) a stored key verification and key exchange module (1)
(b) a Pseudo Random Key Generator (2)
(c) a system of logic circuit elements and interconnections between them
(d) a programmable counter (4)
(e) an open-ended shift register with paralell bit outputs (7)
(f) a pseudorandom Data Generator (11) for supplying surplus data bits
(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the state machine or algorithm status
(h) a serial buffer system 17 for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

9. An encryption and automatic renewal system for confidential E-Mail as in Claim 8, wherein the said circuit block (1) also contains mathematical processing means, for example for adding or deducting a Pass Word from the operative Key number in the key register of said module.

10. An encryption and automatic key renewal system for confidential E-Mail as in any of the aforegoing claims, and / or as shown and described in the accompanying drawings and the Specification.

11. An encryption and automatic encryption key renewal system for confidential E-Mail wherein the output of the said pseudo-random data generator is mixed with the bit levels of other outputs of the encryption circuit or with the clear bit levels of the data flow so as to diffuse any pattern such as may be recognised in the expanded data words.

12. An encryption and automatic key renewal system for confidential E-Mail w h e r e i n the basic functionality of the said algorithm circuit is continually influenced and modified

(a) by the paralell bit outputs of a revolving encryption key register

and (b) by the clear bits of the data inputted to the algorithm circuit for encryption or outputted from the algorithm circuit after decryption.

13. An encryption and automatic key renewal system for confidential E-Mail essentially as characterised in Claim 1 wherein the functionality of the encryption process is broadly determined by an, partly in special hardware executed, algorithm and embodied in a microelectronic chip and wherein this functionality is not rigidly predetermined but continually influenced and modified

(a) by the paralell bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

14. An encryption and automatic key renewal system for confidential E-Mail as characterised in Claim 13 wherein the functionality of the said microelectronic chip circuit is further influenced and modified

(c) by the configuration of a password entered by an operator at the sending and receiving stations in order to ensure that the transmitted text, picture, or voice mail is faithfully reproduced only for those persons who are intended to know it.

15. An encryption and automatic key renewal system for confidential E-Mail as in Claim 13 w h e r e i n the in hardware represented portion of the encryption algorithm also contains memory into which can be written only once, namely when a specific E-Mail station is inaugurated and associated with a definite inauguration date, a definite serial number, and a definite name and a definite Server Station (SSt), and w h e r e i n the said Client Computer (CC) details are also held in memory by the local Server Station (SSt) at an address numvber which is numerically identical with the ID of the CC concerned.

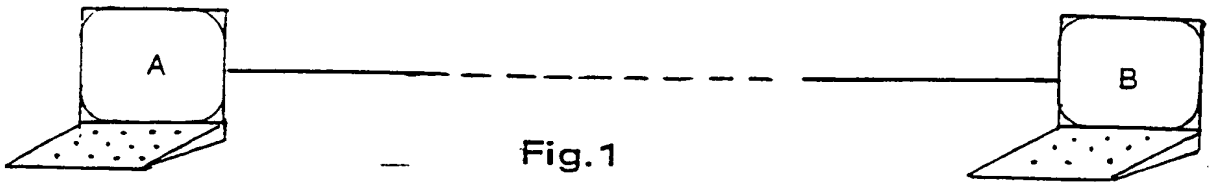


Fig.1

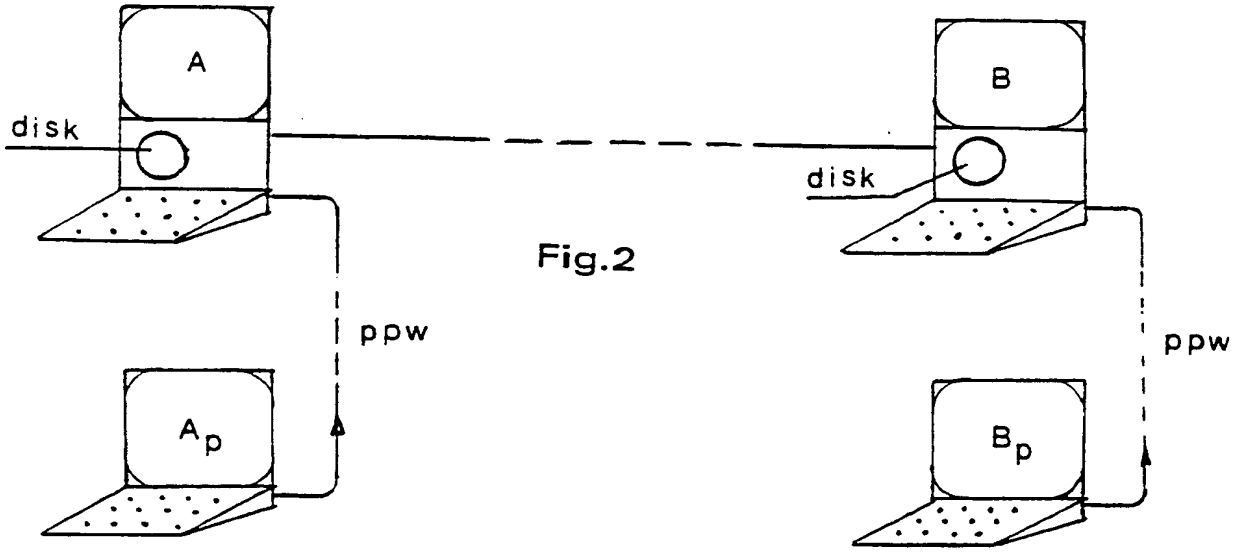


Fig.2

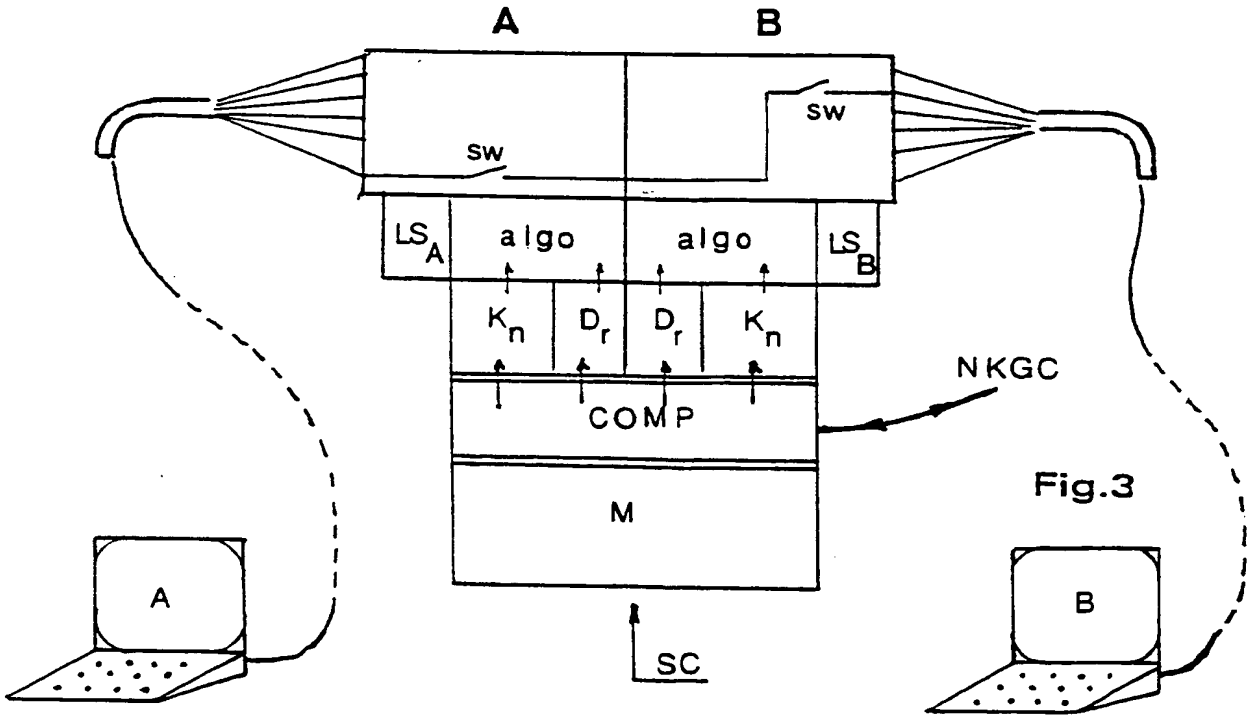
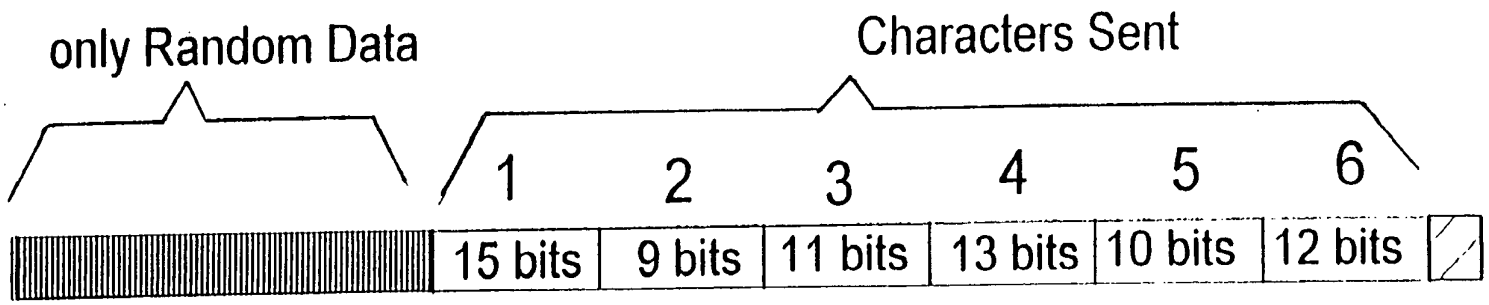


Fig.3

The three modifying components acting together, produce:



The scrambled variable word length data constitute a single message string defying analysis

Fig.4

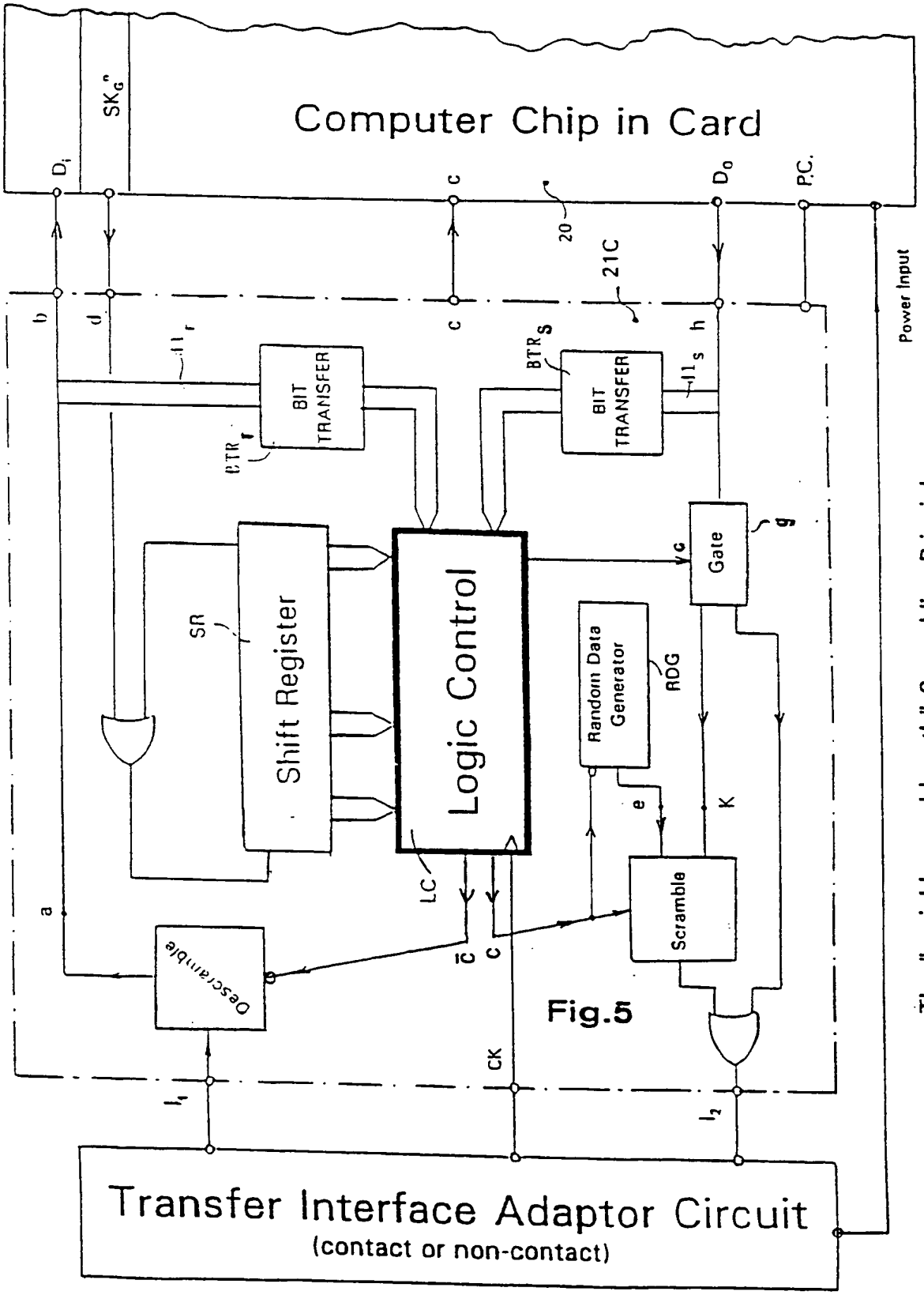


Fig.5

The "variable-word-length" Scrambling Principles
(functional block diagram)

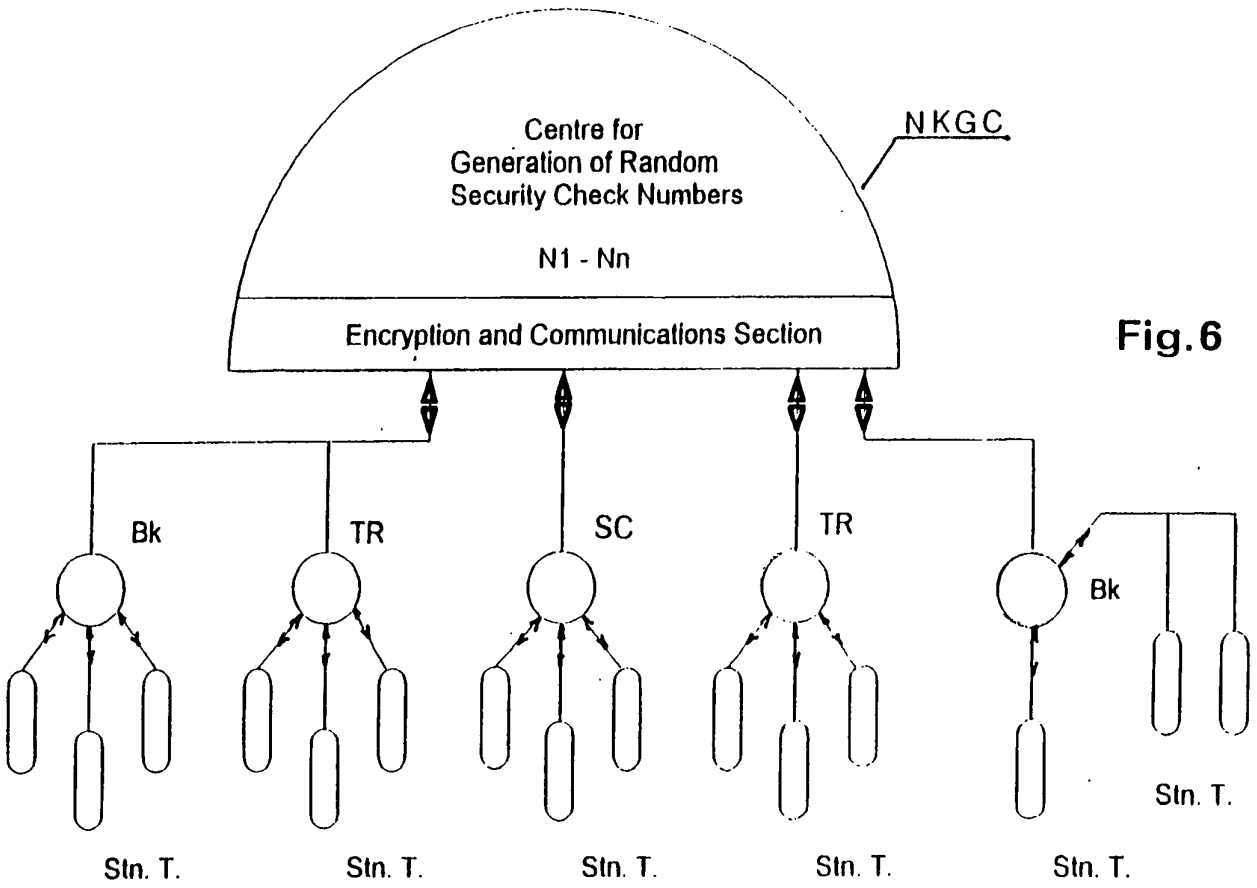


Fig.6

Hierarchical distribution pattern

Bk = bank
TR = transport terminal
Stn.T. = message station terminal

Abandoned Numbers	semi-active numbers					active numbers					Nascent numbers
	10	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	← – – *address register*
	N_{10}	N_9	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	← ——— **number register**
	9	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*10*	← – –
	N_9	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	← ———
	8	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*10*	*9*	← – –
	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	← ———
	7	*6*	*5*	*4*	*3*	*2*	*1*	*10*	*9*	*8*	
	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	
	6	*5*	*4*	*3*	*2*	*1*	*10*	*9*	*8*	*7*	
	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	
	5	*4*	*3*	*2*	*1*	*10*	*9*	*8*	*7*	*6*	
	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	
	4	*3*	*2*	*1*	*10*	*9*	*8*	*7*	*6*	*5*	
	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	
	3	*2*	*1*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	
	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	
	2	*1*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	
	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}	
	1	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	
	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}	N_{19}	

Fig.7 - Surveying the position changes and new entries of check numbers during ten consecutive time periods

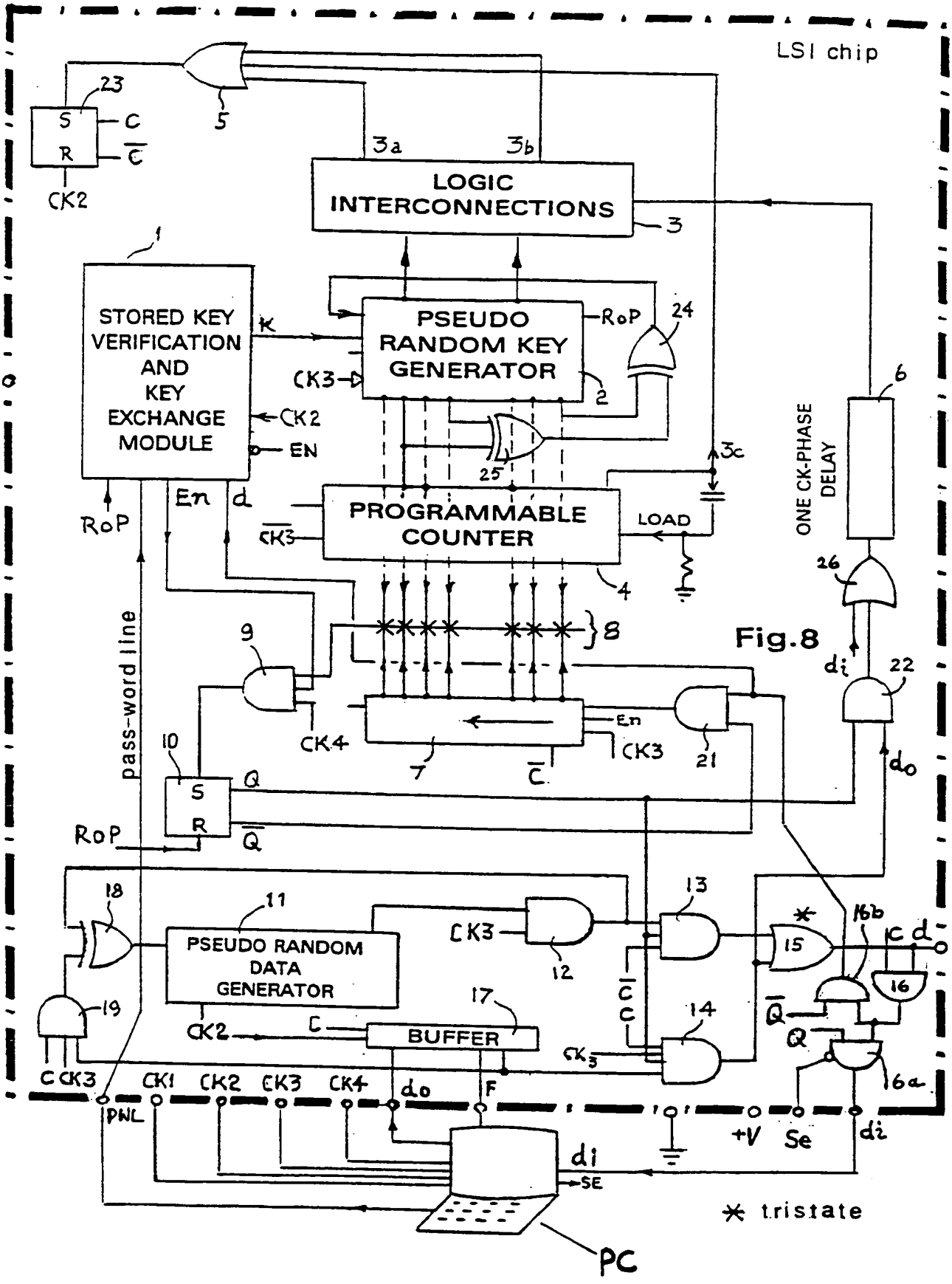

LSI chip
LOGIC INTERCONNECTIONS
STORED KEY VERIFICATION AND KEY EXCHANGE MODULE
PSEUDO RANDOM KEY GENERATOR
PROGRAMMABLE COUNTER
ONE CK-PHASE DELAY
PSEUDO RANDOM DATA GENERATOR
BUFFER
pass-word line
RoP
LOAD
PC
* tristate

Fig.8

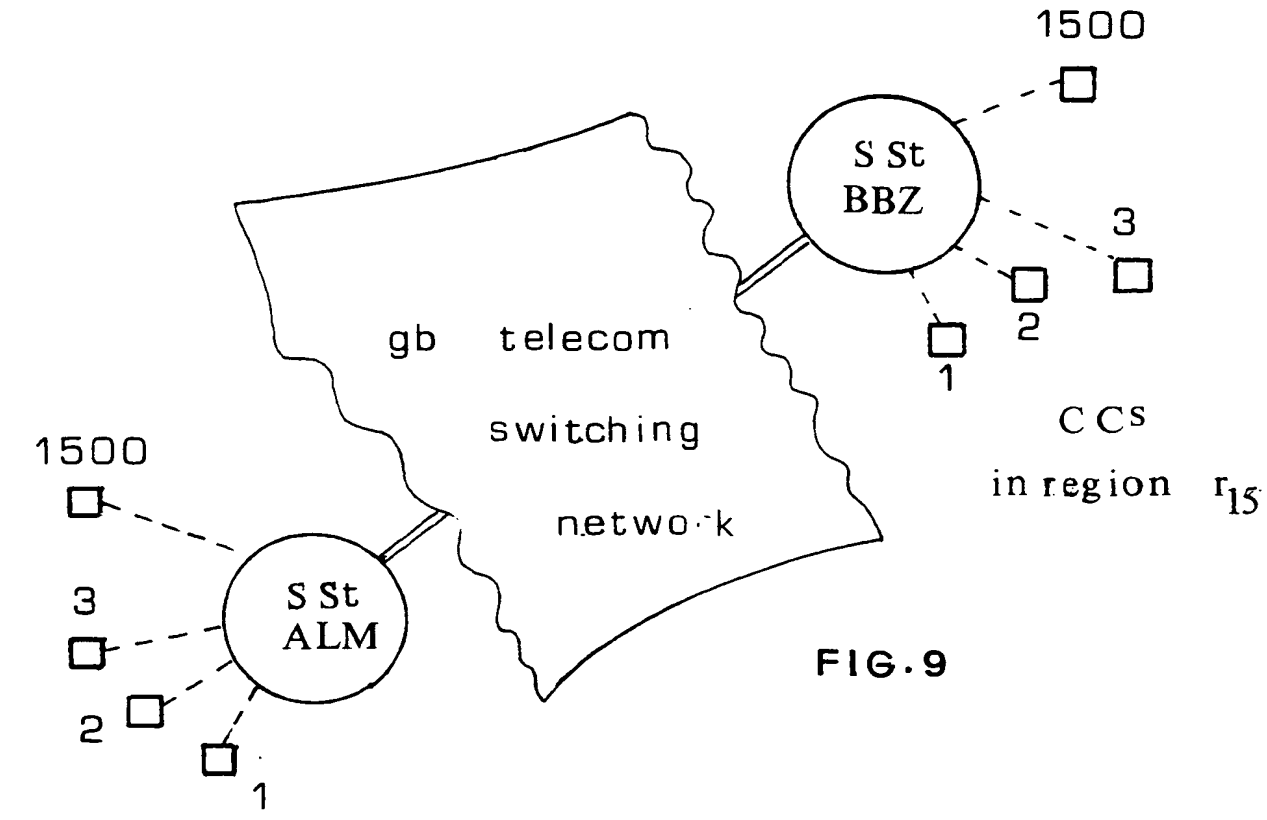

1500
S St
BBZ
3
2
1
gb telecom
switching
network
1500
3
2
1
S St
ALM
CCS
in region r15
CCS
in region r2

FIG.9

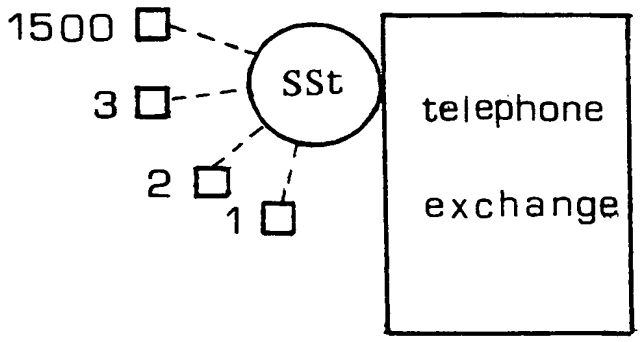

1500
3
2
1
SSt
telephone
exchange

FIG.10

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 29/06

A3

(11) International Publication Number: WO 99/16199

(43) International Publication Date: 1 April 1999 (01.04.99)

(21) International Application Number: PCT/GB98/02881

(22) International Filing Date: 24 September 1998 (24.09.98)

(30) Priority Data:

9720478.8	25 September 1997 (25.09.97)	GB
9820824.2	24 September 1998 (24.09.98)	GB

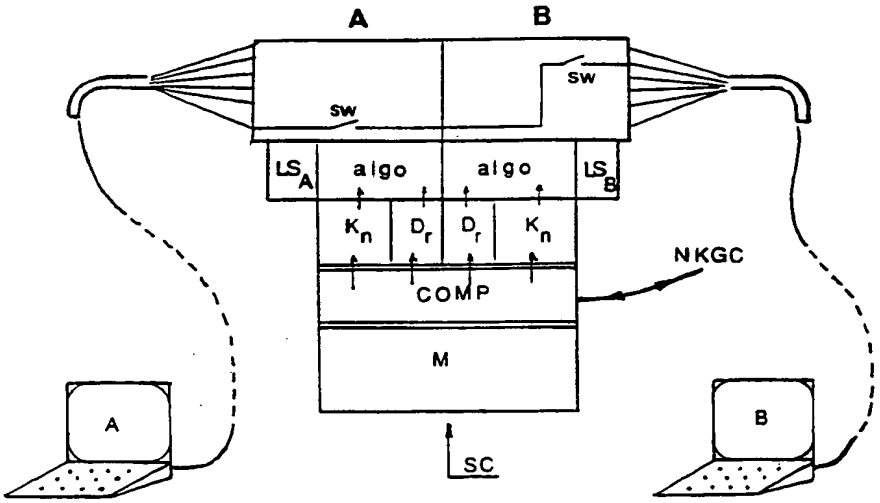
(71)(72) Applicant and Inventor: HALPERN, John, Wolfgang [GB/GB]; 15 Jordan Court, Imgram Crescent W., Hove, East Sussex BN3 5NU (GB).

(81) Designated States: PL, PT, RU, SE, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
21 October 1999 (21.10.99)

(54) Title: A DATA ENCRYPTION SYSTEM FOR INTERNET COMMUNICATION



(57) Abstract

Two versions of a variable word length encryption method are discussed adapted for providing the means for long-term confidential transmission of printed characters, pictures, and voice dialogues over the telephone lines or the internet.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/02881

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAZUE TANAKA ET AL: "KEY DISTRIBUTION SYSTEM FOR MAIL SYSTEMS USING ID-RELATED INFORMATION DIRECTORY" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 10, no. 1, 1 February 1991 (1991-02-01), pages 25-33, XP000209185 ISSN: 0167-4048 page 25, left-hand column, line 1-21 page 26, left-hand column, line 13 - middle column, line 10 page 27, middle column, line 6 - right-hand column, line 17 page 30, middle column, line 7 - page 31, left-hand column, line 8 figure 1 --- -/--	1-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 1999	30/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/02881

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 738 058 A (BARKAN MORDHAY) 16 October 1996 (1996-10-16) abstract column 3, line 29 - column 4, line 5 column 7, line 46-57 column 8, line 3-23 column 9, line 10 - column 11, line 21 column 14, line 37-43 column 16, line 17-48 ---	1-15
A	US 5 412 723 A (CANETTI RAN ET AL) 2 May 1995 (1995-05-02) abstract column 1, line 62 - column 2, line 26 claims 4-6 -----	1-15

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 98/02881

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0738058 A	16-10-1996	US 5864667 A	26-01-1999
US 5412723 A	02-05-1995	EP 0670645 A	06-09-1995
		JP 7250060 A	26-09-1995

A Data Encryption System for Internet Communication

There is a general concensus that serious use of the internet potential for the needs of Commerce and Industry requires a 100% long-term effective system for protecting privacy of the interchanges.
Several aspects apart from privacy would be important in making a choice of the technique. It would have to be suitable for all digital transmissions, irrespective of the coding employed. The same encryption system should be workkable for lettered, audible or visual messages. Also, the time of processing the data should preferably not add more than 80% to the time for transmitting the same data in the clear form. Furthermore, no time should be spent on looking up directories for keys or other procedure rules.

EP-A-0738 058 discloses a system for the secure distribution of encryption keys using a key management device attached to each user's encryption machine, containing a list of secure communication partners and their respective encryption keys. If the desired addressee data is not found in the local data list, the device connects to a secure key distribution centre which is protected by encryption using the public key method.

Kazue Tanake et al: "Key Distribution System for Mail Systems using ID-Related Information Directory", Computers and Security International Journal Devoted to the Study of Technical and Financial Aspects of Computer Security, vol. 10, no. 1 (1991-02-01), pp 25 - 33, ISSD 0167-4048, discloses a key distribution system which uses a public directory, which contains each user's ID-related information. A sender generates a key and key information which depends on the receiver, and sends the key information along with the encrypted message.

The objectives of this patent application follow from what has just been said:

- to create for owners of PC's certain supplementary components easily added with the result of replacing registered and high-priority mail transmissions by a less expensive and faster track protected against breach of confidentiality.
- to reduce the need for personal trustworthiness and to replace it by trustworthiness of the provisions of the system.
- While the idea of "trusted third parties" is appropriate where Government interests are directly involved, the many contingencies that arise when applied to all communications would strain an already overburdened legal system. In contradistinction, the here proposed method would save trustworthy server stations from slipping into arbitrariness, favoritism and self-serving bureaucracy. At the same time it would open a clear route for observers at Govenment level to use their authority of sampling messages in the interest of crime prevention and to do so even for longer periods if and when properly authorized and reasoned for in exposés open for public inspection within six years.

This paper will outline the technical platform for accomplishing the above sketched objectives, with the further provision that its service be available to everyone at a relatively low extra cost over and above the cost of using internet communication.

The said 'technical platform' constitutes a system resting on two main pillars, namely

(a) an algorithm which generates variable wordlength data scrambling

(b) a hierarchic system of key distribution (e.g. a regulated method for ageing and then eliminating keys)

In accordance with a first aspect, the present invention provides an encryption and fully automatic key renewal system for confidential e-mail communication, comprising at least two e-mail stations linked to a communication system; the encryption and automatic key renewal system comprising:

a key generation centre (NKGC) for the generation of random keys for the use of said at least two e-mail stations;

means for the periodic renewal of the keys used by said at least two e-mail stations; and

means for scrambling or encrypting data to be transmitted, using said keys; and

local server stations which store and update said random keys generated in said key generation centre; characterised in that

said local server stations store said keys in a look-up table, each key being associated with an address code and each address code having associated data indicative of the age of said key at any time and to classify the age relative to the age of other keys in use at any given time; and

each said server station including means adapted to issue, prior to each confidential e-mail communication from said at least two e-mail stations, a new key to the sending e-mail station, as the key to be used by said station for scrambling or encrypting the data to be transmitted;

wherein said look-up table means stores a fixed number of encryption key numbers conjointly with their respective access addresses in a shift register-like memory structure wherein the said fixed group of key numbers and said addresses can be moved at quasi randomly arranged times from a younger to an older position the youngest position serving as an entrance point for a new number supplied by the said key generation centre, and the oldest number being relegated to an inactive and reserved position outside the said fixed number or group of encryption keys.

In accordance with an second aspect, there is provided an encryption and automatic encryption key renewal system for confidential e-mail communication, comprising at least one e-mail station linked to a communication system; said system comprising a pseudo-random data generator; characterised by a key generation system and an encryption circuit, said key generation system automatically providing said e-mail station with a new encryption key before each e-mail communication, and wherein the output of said pseudo-random data generator is mixed with the bit levels of outputs of said encryption circuit and with clear bit levels of said input data, according to said key, so as to diffuse any pattern such as may be recognised in the expanded data words.

AMENDED SHEET

In place of a lengthy explanation, we begin by referring to Figure 4 which illustrates the idea of variable word length text transformation. It will be clear that computerised scanning of the encrypted text will in this case have no prospect of providing any clue.

Figure 5 shows a functional block diagram of the encryption/decryption hardware. In early implementations, a 16 bit shift register was used (block SR) with simple output to input connection. The encrypted output resulting from such an arrangement showed a certain periodicity if the clear text consisted of the binary representation of a single letter, for example the letter 'a' in unchanging repetition. This revealed the potential for a certain weakness of the method unless steps are taken to overcome this possible point of attack for a hacker. In present designs we use a 31 bit shift register as the basis for a pseudo random data generator wherein the periodicity is vastly (pattern recurrance only once every 2,14 billion different combinations) reduced. In addition, further measures are taken to begin each message with an undefined length of meaningless text. That text is not delivered in clear by the algorithm. For the user it constitutes simply a few seconds waiting time added to the setting up time. One method of achieving this will be explained in conjunction with Figures 3,4 and 8.

Returning to the description of Fig. 5, paralell outputs from the shift register are connected to various logic elements under the heading LOGIC CONTROL. This comprises for example, a programmable counter, several flip flops and bistables and various gates. Some of the logic control elements are also exposed to inputs of the logic levels of the real data, both outgoing or incoming. These data are applied with a delay of one full clock pulse duration. This is done in the squares named 'bit delay'. The encrypted text on line l_2 is derived from an OR gate into which alternately pass bit elements from the real data and from the Random data generator RDG, respectively a, by real data modified,output from said generator. Encrypted data received are descrambled by action of the Logic Control group, in a single AND gate.

Figures 6 and 7 explain how it is possible to have 8 - 10 simultaneously valid keys and how they are weighted in a number ageing process. Figure 8 shows a functional block diagram of an LSI chip such as would be capable of carrying out data encryption at a high clock rate suitable for any communication network and would provide added security over and above the basic scheme of Figure 5.

AMENDED SHEET

CLAIMS

1. An encryption and fully automatic key renewal system for confidential e-mail communication, comprising at least two e-mail stations linked to a communication system; the encryption and automatic key renewal system comprising:

a key generation centre (NKGC) for the generation of random keys for the use of said at least two e-mail stations;

means for the periodic renewal of the keys used by said at least two e-mail stations; and

means for scrambling or encrypting data to be transmitted, using said keys; and

local server stations which store and update said random keys generated in said key generation centre; characterised in that

said local server stations store said keys in a look-up table, each key being associated with an address code and each address code having associated data indicative of the age of said key at any time and to classify the age relative to the age of other keys in use at any given time; and

each said server station including means adapted to issue, prior to each confidential e-mail communication from said at least two e-mail stations, a new key to the sending e-mail station, as the key to be used by said station for scrambling or encrypting the data to be transmitted;

wherein said look-up table means stores a fixed number of encryption key numbers conjointly with their respective access addresses in a shift register-like memory structure wherein the said fixed group of key numbers and said addresses can be moved at quasi randomly arranged times from a younger to an older position the youngest position serving as an entrance point for a new number supplied by the said key

generation centre, and the oldest number being relegated to an inactive and reserved position outside the said fixed number or group of encryption keys.

2. An encryption and fully automatic key renewal system as in claim 1, wherein the said at least two e-mail stations have means for encrypting and decrypting data including the key numbers themselves, comprising means for executing a key number replacement routine which accepts a new key number only on the basis of a successful completion of the replacement routine, the said routine being implemented prior to the transmission of a new key from the said Key Generation Centre, the said local Server Station (5), and the said e-mail stations.

3. An encryption and automatic key renewal system for confidential e-mail as in claim 1 or 2, comprising means for recognising the legitimacy of a server station by a calling e-mail station, comprising

(a) means for sending to the server station the address code associated with the e-mail station's encrypting key;

(b) means for using the address to assist the server station in obtaining the calling station's encryption key;

(c) the server station comprising equipment to encrypt the key encryption number with itself;

(d) the server station also comprising means to send the encrypted key to the e-mail station;

(e) the e-mail station comprising means for decrypting the received key, using its own key and placing the result into a comparator register, and means for determining if the compared numbers are equal for informing the server station accordingly.

4. An encryption and automatic key renewal system for

AMENDED SHEET

confidential e-mail as in claim 3, wherein in the case that the compared numbers are equal the server station is programmed to obtain from its storage means an alternative key number (K_c) from the currently stored key numbers, and to encrypt that new number with the key of the calling station, and wherein the latter is programmed upon receipt of the encrypted new key to decrypt said number and to place it into its key register in substitution of the number it had before.

5. An encryption and automatic key renewal system for confidential e-mail as in claim 3, wherein the server station (SC) also acts as an switchboard for connecting a calling station (A) to a requested receiving station (B), and wherein the server station consists of a computer section (COMP) and a twin structure which is equipped with two sets of encryption algorithm (algo) , two sets of switching controls, (LSA and LSB), and two sets of buffer memories (K_n) for holding key number, address codes and other relevant flags as supplied by the computer section (COMP).

6. An encryption and automatic key renewal system for confidential e-mail s in claim 5, wherein the said server station (SC) also contains a pseudo-random generator register (D_r) in order to generate quasi-data inputs of equal length simultaneously transmitted and encrypted by the said alternative key number (K_c) to the communicating stations (A, B) in order thereby to shift the starting conditions in the algorithms of the e-mail units for the real text to an undetectable point.

7. An encryption and automatic key renewal system for confidential e-mail as in claim 5 or 6, wherein the algorithms used for the encrypting process produce word-bit configurations consisting of more than 8 bits and less than 16 bits per word transmitted, and the bit

number per word is continually changing.

8. An encryption and automatic key renewals system for confidential e-mail as in claim 6, wherein the precise point in time for switching the communicating stations from the said initial meaningless random information is functionally defined by comparing the data flow in two registers, namely register (2) with that of register (7) whereby the data shift is prompted by the same clock phase (CK3) but occurs in opposite directions.

9. An encryption and automatic key renewal system for confidential e-mail as in any of the preceding claims, comprising

(a) a stored key verification and key exchange module (1),

(b) a Pseudo Random Key Generator (2),

(c) a system of logic circuit elements and interconnections between them

(d) a programmable counter (4)

(e) an open-ended shift register with parallel bit outputs (7)

(f) a pseudo-random Data Generator (11) for supplying surplus data bits

(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the state machine or algorithm status)

(h) a serial buffer system (18) for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

10. An encryption and automatic renewal system for confidential e-mail as in claim 9, wherein the said module (1) also contains mathematical processing means for adding or deducting a password from the operative key number in the key register of said module.

AMENDED SHEET

11. An encryption and automatic renewal system as claimed in any preceding claim, wherein said data to be encrypted is encrypted using a variable word length encryption system, wherein the data output from the encryption system comprises random data bits and real data bits, said real data bits being transmitted at a randomly varying rate, according to the key being used by said e-mail station.

12. In an encryption and fully automatic key renewal system, a key replacement routine comprises the steps of

in an automatic server station: receiving from a calling station a stored encryption key access address in clear text and in encrypted form the e-mail number of the party to be called,

based on said access address, identifying the encryption key which had been allocated to the calling station for its preceding confidential e-mail communication,

based on said identified key, the automatic server station encrypts the key by itself and adds a quasi random check number in encrypted form, and sends both to the calling station,

the calling station compares the decrypted received key with the one stored, and, if not identical, provides and indication thereof,

the automatic server station receives from the e-mail station the decrypted check number and compares it with the check number used before encrypting it, and, if not the same, will not proceed, and if the same, will decrypt the access number of the called station, and execute the call repeating the verification steps carried out with the calling station.

13. An encryption and automatic encryption key renewal system for confidential e-mail communication, comprising at least one e-mail station linked to a communication

AMENDED SHEET

system; said system comprising a pseudo-random data generator; characterised by a key generation system and an encryption circuit, said key generation system automatically providing said e-mail station with a new encryption key before each e-mail communication, and wherein the output of said pseudo-random data generator is mixed with the bit levels of outputs of said encryption circuit and with clear bit levels of said input data, according to said key, so as to diffuse any pattern such as may be recognised in the expanded data words.

14. An encryption and automatic key renewal system as claimed in claim 13, wherein the operation of said encryption circuit is continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by the clear bits of the data inputted to the encryption circuit for encryption or outputted from the encryption circuit after decryption.

15. An encryption and automatic key renewal system for confidential e-mail as claimed in any of claims 1 to 11, 13 or 14, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

16. An enoryption and automatic key renewal system for confidential e-mail as characterised in claim 14,

AMENDED SHEET

wherein the functionality of the said microelectronic chip circuit is further influenced and modified

(c) by the configuration of a password entered by an operator at the sending and receiving stations in order to ensure that the transmitted text, picture or voice mail is faithfully reproduced only for those persons who are intended to know it.

17. An encryption and automatic key renewal system for confidential e-mail as in claim 15 wherein means for carrying out the encryption process includes a memory into which can be written only once, namely when a specific e-mail station is inaugurated and associated with a definite inauguration date, a definite serial number, and a definite name and a definite server station (SC), and wherein the said client computer (CC) details are also held in memory by the local server station (SSt) at an address number which is numerically identical with the ID of the CC concerned.